International Journal of Physical and Social Science
Vol. 9 Issue 7, July 2019
ISSN: 2249-5894 Impact Factor: 6.644
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

CELL PHONE CLONING: TECHNIQUES, PREVENTIONS AND SECURITY MEASURES

Vibhor Mohan*

Abstract

To say that mobile (cellular/cell) phones have become the integral part of modern lifestyle would be an understatement. This latest mode of communication is considered as most significant as it involves '3e's - ease of use, economic and efficient. But with introduction of internet-enabled services on 'smart' phones, the data stored therein has become the new target that miscreants would like to use for frauds, or to breach the phone owner's privacy. General ignorance about the threat of this new menace called 'Mobile Phone Cloning' makes us all the more vulnerable to fall prey to data thieves on the prowl. Even the available advanced security mechanisms many not be very effective at times. So if you have always worried about physically losing your handset, the threat to cloning should not be taken lightly either. On simple symptom to detect mobile cloning is sudden shooting up of bills. It could be an indication that another cell phone has been turned into an exact replica of the original cell phone like a clone, without the owner having the slightest idea. Among other dangers, while calls can be made from both phones, only the original is billed. This paper delves deeper into the whole phenomenon of mobile phone cloning, its implementation in Global System for Mobile communication (GSM) and Code Division Multiple Access (CDMA) phones, and most importantly, ways of keep cell phones safe from this monster called cloning. The possible future threats related to the problem have also be taken into account.

Keywords:
GSM; CDMA; ESN; Mobile Identification Number; SCN (Station Class Mark)

* School of Communication Studies at Panjab University, Chandigarh

1. Introduction

Mobile communication penetration has been growing from the cities into the remotest of rural areas and smart phones are being used to carry out business deals on the go these days. A typical cell phone with basic applications provides valuable services to its users who are willing to pay a considerable premium over a fixed line phone, to be able to walk and talk freely.

As per a recent report by the Internet and Mobile Association of India (IAMAI) and IMRB International, India had 205 million Internet users in October, 2013. Out of the total Internet users, 110 million users accessed Internet from mobile devices with 25 million users from rural areas. And with growing mobile usage, threat of cloning too is increasing. Tech2.in.com claims that 1,300 cases of IMEI cloning found in India between 2009-2012. There are numerous freeware software available for sniffing, thrashing and cloning of cell phone and it takes less than an hour to program, changing of EEPROM and reassembling

Across the globe, instant communication is available with computers, emails, internet, and cell phones. But it is the mobile phones that have increasingly become something of a household item in the past few decades. Launched to facilitate communication in all places and at all times, cell phones have developed into sophisticated gadgets offering numerous prospects. [1]

It was the Dolly the lamb clone that first made mobile phone manufacturers and scientists wake up to the issue and take note of the problem. Mobile phone users are under a consant threat of harmful cloning. Millions of mobile phones users, be it GSM or CDMA, run at risk of having their phones cloned. Unfortunately, there is no way the subscriber can detect cloning. Events like call dropping or anomalies in monthly bills can act as tickers. [2]

Unfortunately, the advance of security standards has not kept pace with the dissemination of mobile communication. Some of the features of mobile communication make it an alluring target for criminals. It is a relatively new invention, so not all people are quite familiar with its possibilities, in good or in bad. Its newness also means intense competition among mobile phone service providers as they are attracting customers. It is also known as cell phone piracy and has been taking place throughout the world since decades.

The most worrying aspect of the problem is that there is not much that the cell phone user can do to prevent this. Such a crime first came to light in January 2005 when the Delhi police arrested a person with 20 cell phones, a laptop, a SIM scanner, and a writer. The accused was running an exchange illegally wherein he cloned CDMA-based mobile phones. He used software for the cloning and provided cheap international calls to Indian immigrants in West Asia. A similar racket came to light in Mumbai resulting in the arrest of four mobile dealers.

2. History of cell phone cloning

The early 1990s were boom times for eavesdroppers. Any curious teenager with a £100 Tandy Scanner could listen in to nearly any analogue mobile phone call. As a result, Cabinet Ministers, company chiefs and celebrities routinely found their most intimate conversations published in the next day's tabloids Cell phone cloning started with Motorola "bag" phones and reached its peak in the mid 90's with a commonly available modification for the Motorola "brick" phones, such as the Classic, the Ultra Classic, and the Model 8000. [3]

3. **Common techniques used in phone cloning**

Cloning of a cell phone occurs when the account number of a victim telephone user is stolen and reprogrammed into another cellular telephone. [13]

Cloning involved modifying or replacing the Electrically Erasable Programmable Read-Only Memory (EEPROM) in the phone with a new chip which would allow you to configure an ESN (Electronic serial number) via software. Each cellular phone has a unique pair of identifying numbers: the electronic serial number (“ESN”) and the mobile identification number (“MIN”). The ESN/MIN pair can be cloned in a number of ways without the knowledge of the carrier or subscriber through the use of electronic scanning devices. After the ESN/MIN pair is captured, the cloner reprograms or alters the microchip of any wireless phone to create a clone of the wireless phone from which the ESN/MIN pair was stolen. The entire programming process takes ten minutes per phone. After this process is completed, both phones (the legitimate and the clone) are billed to the original, legitimate account. [14]

Cellular data thieves can capture ESN/MINs using devices such as cell phone ESN reader or digital data interpreters (DDI). DDIs are devices specially manufactured to intercept ESN/MINs. By simply sitting near busy roads where the volume of cellular traffic is high, cellular thieves monitoring the radio wave transmissions from the cell phones of legitimate subscribers can capture ESN/MIN pair.

Numbers can be recorded by hand, one-by-one, or stored in the box and later downloaded to a computer. ESN/MIN readers can also be used from inside an offender's home, office, or hotel room, increasing the difficulty of detection.

To reprogram a phone, the ESN/MINs are transferred using a computer loaded with specialised software, or a “copycat” box, a device whose sole purpose is to clone phones. The devices are connected to the cellular handsets and the new identifying information is entered into the phone. There are also more discreet, concealable devices used to clone cellular phones. Plugs and ES-Pros which are about the size of a pager or small calculator do not require computers or copycat boxes for cloning. The entire programming process takes ten-15 minutes per phone.

The cellular telephone industry does not charge legitimate, victimized customers for fraudulent calls; rather the companies absorb the losses themselves. In addition to losses due to fraudulent billing, the cellular companies incur losses due to the fees paid for connections and long-distance charges.[4]

Cloning still works under the AMPS/NAMPS system, but has fallen in popularity as older clone able phones are more difficult to find and newer phones have not been successfully reverse-engineered. Cloning has been successfully demonstrated under GSM, but the process is not easy and it currently remains in the realm of serious hobbyists and researchers. [5]

4. How big is the threat of cloning?

Each year, the mobile phone industry loses millions of dollars in revenue because of the criminal actions of persons who are able to reconfigure mobile phones so that their calls are billed to other phones owned by innocent third persons. Often these cloned phones are used to place hundreds of calls, often long distance, even to foreign countries, resulting in thousands of dollars in air time and long distance charges. Cellular telephone companies do not require their customers to pay for any charges illegally made to their account, no matter how great the cost. But some portion of the cost of these illegal telephone calls is passed along to cellular telephone consumers as a whole.

Many criminals use cloned cellular telephones for illegal activities, because their calls are not billed to them, and are therefore much more difficult to trace.

This phenomenon is especially prevalent in drug crimes. Drug dealers need to be in constant contact with their sources of supply and their confederates on the streets. Traffickers acquire cloned phones at a minimum cost, make dozens of calls, and then throw the phone away after as little as a days' use.

In the same way, criminals who pose a threat to our national security, such as terrorists, have been known to use cloned phones to thwart law enforcement efforts aimed at tracking their whereabouts.

5. Detection and prevention of cloning

While research may still be on to make mobile phone data completely out of bounds for thieves, there are some lessons that can be learnt from the past to read the signs of cloning well in time and plug the breach to save vital information that could be misused if it falls in wrong hands.
Here are some effective ways to detect the cloning.

(a) ***Duplicate Detection:***

If the service provider finds out the traces of the same phone in at several places at a time, then it should shut down the complete network. If the network is down, the legitimate user will respond back to the service provider and the ESN/ MIN can be reprogrammed. The fraudulent user will be automatically bypassed. The only pitfall in this system is that it is very much difficult for the service provider to trace out the duplicates.

(b) ***Velocity Trap:***

If the location of the phone is continuously changing or the location is too far away from last call in impossible amount of time, then it falls under velocity trap. For example, if first call is made from Mumbai and another is made from Bangalore within 15 minutes, or if the calls are made from Dadar and Virar within 5 minutes, Velocity Trap is encountered.

(c) ***RF (Radio Frequency):***

Radio fingerprinting is a process that identifies a cellular phone or any other radio transmitter by the unique "fingerprint" that characterizes its signal transmission. An electronic fingerprint makes it possible to identify a wireless device by its unique radio transmission characteristics. Radio fingerprinting is commonly used by cellular operators to prevent cloning of cell phones. A cloned cell phone will have a same numeric equipment identity but a different radio fingerprint. If the service provider spots the same fingerprint of one existing unit, it temporarily suspends the service.

(d) ***Usage Profiling*****:**

The usage patterns of the users too can be studied to detect cloning. If any discrepancies are noticed, the customer is contacted. For example, if a legitimate user is normally accustomed to the local calls and rarely STD calls, and if a call is traced suddenly to foreign country, then there can be chance of cloning.

(e) ***Call Counting*****:**

Each phone records the logs of the service utilized. Each service provider also keeps the same logs. If the logs from the company and subscriber are different, then the only conclusion is that the phone is cloned

(f) ***PIN Codes:***

The service provider can assign a smart PIN (Personal Identification Number) code to each user. Before calling, the user will request for service privilege from service provider. After the call user will again ask for temporary suspension of service. This PIN can be shared only by user and company. The security algorithms, encryption standards can be implemented on this PIN rather than ESN/MIN Pair. [12]

6. Creating a GSM clone

A digital cellular phone technology based on TDMA GSM phones use a Subscriber Identity Module (SIM) card that contains user account information. Any GSM phone becomes immediately programmed after plugging in the SIM card, thus allowing GSM phones to be easily rented or borrowed. Operators who provide GSM service are Airtel, Idea etc.

The flaws is in the comp 128 authentication algorithm used as instantiation of a3/a8 used by GSM providers. Attackers attack the algorithm by using a chosen challenge attack and querying the SIM card for each one. Analyzing the responses from these queries they determine the value of secret key used for authentication. Software required for this are Cardinal Sim Editor, CardMaster, Emulator SIMEMU etc.

Bluebugging is the process of sniffing communication from a bluetooth-enabled cell phone. Bsscanner is also used for sniffing bluetooth devices. [6]

In the telecommunications security field, openness is critical to good design. Codemaking is so hard to get right the first time that it is crucial to have others double-check one's ideas. Instead, the GSM design committee kept all security specifications secret -- which made the information just secret enough to prevent others from identifying flaws in time to fix them, but not secret enough to protect the system against eventual scrutiny. With 80 million GSM users, fixing flaws in such a widely-fielded system is likely to be quite costly.

Fixing the flaw may potentially be expensive. A new authentication algorithm would have to be selected. Then new SIMs would have to be programmed with the new algorithm, and distributed to the 80 million end users. Finally, a software upgrade may be required for all authentication centers. [7]

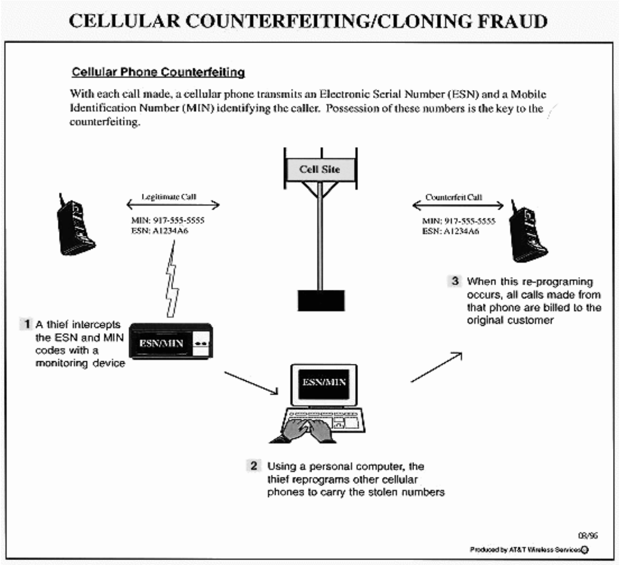
7. Creating CDMA clone

A method for transmitting simultaneous signals over a shared portion of the spectrum. There is no Subscriber Identity Module (SIM) card unlike in GSM. Operators who provides CDMA service in India are Reliance and Tata Indicom.

The CDMA Fraternal Clone method will allow the forensic examiner/analyst to transfer all user-created files and current settings from one CDMA phone into another, so that the target phone (CDMA Fraternal Clone) can be examined. The CDMA Fraternal Clone is used as a vehicle to view the user created data and settings from the original phone in their native format. The CDMA Fraternal Clone process allows the forensic examiner/analyst to view and work with the extracted data in a way that emulates the original phone.

In order to successfully complete the CDMA Fraternal Clone process, the following hardware and software is necessary: Forensic computer, Correct USB Cable and drivers for the CDMA phone, A CDMA phone of same make, model, and firmware version of original phone 2, Cell phone software/equipment capable of extracting or creating an image of the file system of the CDMA phone such as BitPim,3 Paraben's Device Seizure, or Cellebrite.

The process of creating a CDMA Fraternal Clone phone consists of four phases: (1) preparation of the forensic machine and the target phone; (2) creation of a full copy of the file structure of the evidentiary phone; (3) transfer of the data extracted from the evidentiary phone to the target phone to create the CDMA Fraternal Clone, and (4) verification of the integrity of the data transferred from the evidence phone to the CDMA Fraternal Clone. [8]


CELLULAR COUNTERFEITING/CLONING FRAUD
Cellular Phone Counterfeiting
With each call made, a cellular phone transmits an Electronic Serial Number (ESN) and a Mobile Identification Number (MIN) identifying the caller. Possession of these numbers is the key to the counterfeiting.
Cell Site
Legitimate Call
MIN: 917-555-5555
ESN: A1234A6
Counterfeit Call
MIN: 917-555-5555
ESN: A1234A6
1 A thief intercepts the ESN and MIN codes with a monitoring device
ESN/MIN
ESN/MIN
2 Using a personal computer, the thief reprograms other cellular phones to carry the stolen numbers
3 When this re-programing occurs, all calls made from that phone are billed to the original customer
08/96
Produced by AT&T Wireless Services

There are various cloning software available some of them are free while some are paid.

- **Keriver Disk Sync** is an easy-to-use but powerful disk/partition cloning tool, which can sync/clone a disk or partition to another disk or partition directly.
- **MiniTool Drive Copy** is a Free Disk Copy Software and Disk Cloning tool.
- **Simcard Data Salvage Program** Mobile phone SIM card information recovery software is an advance utility to recover deleted inbox, outbox, sent and draft SMS from inaccessible mobile phone SIM card. [11]
- **Patagonia** is software available in the market which is used to clone CDMA phones. Using this software a cloner can modify the ESN/MIN of any CDMA phone.
- **Device Seizure, GSM.xry, TULP2G, SecureView** etc. [9]

8. Security and Countermeasures

The security services provided by GSM are Anonymity, *Authentication, Signaling Protection and User Data Protection.* The objective of security for GSM system is to make the system as secure as the public switched telephone network. The use of radio at the transmission media allows a number of potential threats from eavesdropping the transmissions. The technical features for security are only a small part of the security requirements; the greatest threat is from simpler attacks such as disclosure of the encryption keys, insecure billing systems or corruption. A balance is required to ensure that these security processes meet these requirements. [12]

The countermeasures are designed:

- to make the radio path as secure as the fixed network, which implies anonymity and confidentiality to protect against eavesdropping;
- to have strong authentication, to protect the operator against billing fraud;
- to prevent operators from compromising each others' security, whether inadvertently or because of competitive pressures.

There are some commercial systems on the market that can provide these features. These 'Fraud Engines' enable patterns in billing data to be analysed, and give time for swift effective action. With fraud detection capability, and security procedures in place, it is possible to minimise the effect of fraud on a billing system.[10]

*8.1 **Ways to prevent cloning***

- User verification using PIN(Personal Identification Number)
- Blacklisting of stolen phones
- Traffic analysis
- Electrically checking the ESN/MIN
- Confidential information should never be saved in mobiles.
- A password protected phone locking system may prevent the cloning to certain extent.
- All devices should be covered by a company policy.[11]

9. Conclusion

To conclude, cell phone communication is one of the most reliable, efficient and widespread. The usage of the system can be changed in either constructive or destructive ways. Unfortunately the security standards are quite easy to breach and takes very less amount of time. Moreover, cloning methodology is widespread and can be implemented easily. Hence, it must be considered that the security system which was implemented lately must not be fruitful enough to secure the system in future. Therefore it is absolutely important to verify the working of a protection system over a precaution system every once a while and change or update it every once a year. To avoid such abuse to telecommunication system it is absolutely necessary to check out the weakness and vulnerability of existing telecom systems. If it is planned to invest in new telecom equipment, a security plan should be made and the system should be tested before being implemented.

References

[1] Manjush Talmale, Abhishek Kinhekar, Akshay Saraf, Milind Bhajan (2013), "Mobile Phone Cloning: History, Present Scenario and Precautionary Techniques", IJAIEM)

[2] Faiz Jahangir, Rizwan Khan (2014), "MOBILE PHONE CLONING", VSRD International Journal of Computer Science & Information Technology, Vol. IV , Issue I January 2014, pp 13-16.

[3] Sharmasoni, (2012), "Mobile Phone Cloning", Http://www.studymode.com/essays/Mobile-Phone-Cloning-1054219.html

[4] Cellular Telephone Cloning Final Report Economic Crimes Policy Team United States Sentencing Commission January 25, 2000

[5]Mobile Phone Cloning : Seminar Report and PPT

[6] http://www.techmantras.com/content/gsm-mobile-hacking-using-sim-cloning

[7] http://www.isaac.cs.berkeley.edu/isaac/gsm.html

[8] Murphy, C. "The fraternal clone method for CDMA cell phones." *Small Scale Digital Device Forensics Journal* 3.1 (2009): 1-8.

[9] Goel, Aaruni, Madhup Sharma, and Paresh Pathak.(2012), "The Approaches to Prevent Cell Phone Cloning In Cdma Enviornment." *International Journal of Computer Applications* 45.

[10] http://www.brookson.com/gsm/gsmdoc.htm

[11] http://download.sharewarecentral.com/28/98946/minitool-drive-copy.html

[12] Mirela Sechi, Moretti Annoni Notare, " Wireless Communications: SECURITY MANAGEMENT AGAINST CLONING MOBILE PHONES"

[13] http://en.wikipedia.org/wiki/Phone_cloning

[14] Kessler, G. (2010). Cell Phone Analysis: Technology, Tools, and Processes. Mobile Forensics World. Chicago: Purdue University.

[15] Mislan, R.P., Casey, E., & Kessler, G.C. (2010). The Growing Need for On-Scene Triage of Mobile Devices. Digital Investigation, 6(3-4), 112-124